Third-Party and Vendor Risk Management (TPRM) Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

Third-Party Risk Management has rapidly evolved from a mere compliance checkbox into a strategic imperative for organizational resilience in the digital era. With the increasing reliance on global supply chains and cloud services, the expanded attack surface necessitates a robust, risk-based approach to managing external relationships. Recent high-profile data breaches and supply chain attacks have underscored that a vendor's vulnerability directly impacts the client organization's cybersecurity posture, regulatory compliance, and ultimately, its reputation. This critical course provides the essential framework and best practices to proactively identify, assess, mitigate, and continuously monitor risks across the entire vendor lifecycle.

Third-Party and Vendor Risk Management (TPRM) Training Course is designed to empower risk, compliance, and procurement professionals to build and mature an integrated TPRM program. We will move beyond traditional checklist-based due diligence to focus on continuous monitoring, risk tiering, and leveraging automation and predictive analytics to manage emerging risks like ESG and geopolitical risk. Participants will gain mastery over the core components of the TPRM lifecycle, from initial vendor vetting and contractual safeguards to incident response and secure offboarding. Mastering these skills is vital to safeguard sensitive data, ensure business continuity, and maintain regulatory alignment in today's complex, interconnected business ecosystem.

Programme Curriculum

Third-Party and Vendor Risk Management (TPRM) Training Course

Introduction

Third-Party Risk Management has rapidly evolved from a mere compliance checkbox into a strategic imperative for organizational resilience in the digital era. With the increasing reliance on global supply chains and cloud

services, the expanded attack surface necessitates a robust, risk-based approach to managing external relationships. Recent high-profile data breaches and supply chain attacks have underscored that a vendor's vulnerability directly impacts the client organization's cybersecurity posture, regulatory compliance, and ultimately, its reputation. This critical course provides the essential framework and best practices to proactively identify, assess, mitigate, and continuously monitor risks across the entire vendor lifecycle.

Third-Party and Vendor Risk Management (TPRM) Training Course is designed to empower risk, compliance, and procurement professionals to build and mature an integrated TPRM program. We will move beyond traditional checklist-based due diligence to focus on continuous monitoring, risk tiering, and leveraging automation and predictive analytics to manage emerging risks like ESG and geopolitical risk. Participants will gain mastery over the core components of the TPRM lifecycle, from initial vendor vetting and contractual safeguards to incident response and secure offboarding. Mastering these skills is vital to safeguard sensitive data, ensure business continuity, and maintain regulatory alignment in today's complex, interconnected business ecosystem.

Course Duration

5 days

Course Objectives

Upon completion of this course, participants will be able to:

1. Design and Implement a comprehensive, risk-based TPRM Framework aligned with enterprise risk strategy.
2. Navigate the Regulatory Landscape, including the impacts of GDPR, HIPAA, PCI DSS, and the SEC Cybersecurity Rule on third-party relationships.
3. Execute thorough Vendor Due Diligence and Risk Assessment procedures based on a tiered approach.
4. Master the principles of Risk Tiering and Vendor Criticality to prioritize high-impact third parties effectively.
5. Identify and classify the spectrum of risks, including Cybersecurity Risk, Operational Risk, Compliance Risk, Financial Risk, and Reputational Risk.
6. Develop robust Contractual Safeguards and Service Level Agreements (SLAs) to enforce security and performance expectations.
7. Implement Continuous Monitoring strategies utilizing Security Ratings and automated tools for real-time risk visibility.
8. Integrate Fourth-Party Risk Management to assess the security and compliance of sub-processors and subcontractors.
9. Address Emerging Risks by incorporating ESG and Geopolitical Risk factors into vendor evaluations.
10. Formulate an effective Third-Party Incident Response Plan and manage the lifecycle of a vendor-related security breach.
11. Conduct a secure and structured Vendor Offboarding process to mitigate residual access and data risks.
12. Define key TPRM Performance Metrics and implement effective risk Reporting and Communication for executive stakeholders.
13. Leverage TPRM Automation and Integrated Risk Management platforms to enhance program scalability and efficiency.

Target Audience

1. Risk & Compliance Officers (CROs, CCOs)
2. Procurement & Sourcing Managers

3. Third-Party Risk Management (TPRM) Specialists
4. Information Security & IT Risk Managers
5. Internal & External Auditors
6. Legal and Contract Management Teams
7. Business Continuity & Resilience Managers
8. Vendor Managers & Relationship Owners

Course Modules

Module 1: The TPRM Foundation and Strategic Imperative

- Defining TPRM, the vendor lifecycle, and the expanded attack surface.
- The spectrum of third-party risks.
- Establishing a Risk Appetite and defining the core components of an Integrated TPRM Framework.
- Case Study: Analyzing the SolarWinds Attack to understand the severity and scope of a sophisticated supply chain compromise.
- Defining roles, responsibilities, and ensuring Executive Sponsorship and cross-functional collaboration.

Module 2: Vendor Identification, Risk Tiering, and Initial Due Diligence

- Creating a comprehensive and up-to-date Vendor Inventory and managing "Shadow IT."
- Methodologies for Risk Tiering based on Vendor Criticality, data access, and operational impact.
- Developing and deploying effective, risk-adjusted Due Diligence Questionnaires
- Case Study: Reviewing the Target Data Breach via an HVAC vendor to illustrate failure in initial vendor vetting and segmentation.
- Assessing vendor financial health, licensing, and Business Continuity/Disaster Recovery plans.

Module 3: Deep Dive into Risk Domains and Assessments

- Conducting Information Security and Cyber Risk Assessments
- Assessing Data Privacy Compliance against global standards like GDPR and CCPA.
- Evaluating ESG Risk and Geopolitical Risk.
- Case Study: Examining a hypothetical Data Leak Scenario due to a cloud provider's lax data destruction policies to identify non-compliance penalties.
- Managing Fourth-Party Risk by ensuring sub-processors meet organizational standards and are addressed in contracts.

Module 4: Contractual Safeguards and Negotiation

- Establishing mandatory Security Requirements and Data Protection Clauses within vendor contracts.
- Negotiating and defining rigorous Service Level Agreements, particularly for critical services.
- Including clauses for Right to Audit, Breach Notification Timelines, and Indemnification.
- Case Study: Analyzing a flawed contract that lacked adequate Incident Reporting requirements, leading to delayed breach disclosure and fines.
- Best practices for using standardized contracts and integrating TPRM findings into the final agreement.

Module 5: Continuous Monitoring and Performance Management

- Shifting from periodic assessments to Continuous Monitoring for real-time risk intelligence.
- Utilizing Security Ratings Services and threat intelligence feeds to track vendor security posture.
- Monitoring Performance Metrics and adherence to contractual SLAs.

- Case Study: Demonstrating the use of SecurityScorecard or similar platforms to automatically detect a vendor's public-facing security deterioration.
- Implementing a formal Remediation and Exception Management process for identified control gaps.

Module 6: Incident Response and Crisis Management

- Developing a Third-Party Incident Response Plan and integrating it with the enterprise BCDR plan.
- Defining clear roles, responsibilities, and Communication Protocols during a vendor security incident.
- Managing the legal and regulatory obligations for Breach Notification
- Case Study: Analyzing the Capital One Data Breach via a former AWS employee to understand the non-delegable responsibility and regulatory fines.
- Post-incident activities: Root Cause Analysis, lessons learned, and required contractual actions.

Module 7: Program Maturity, Automation, and Tooling

- Assessing the Maturity of the current TPRM program using established models
- Leveraging TPRM Automation and AI/Machine Learning for intelligent Risk Triage and workflow streamlining.
- Evaluating and selecting appropriate GRC/TPRM Software Solutions and platforms.
- Case Study: Simulating the implementation of a new TPRM Automation Tool to reduce vendor onboarding time from weeks to days.
- Strategies for integrating TPRM data with other enterprise systems

Module 8: Managing the End-of-Relationship

- Establishing a formal and structured Vendor Offboarding and Termination Strategy.
- Ensuring the secure return or certified destruction of all Sensitive Data and intellectual property.
- Revoking all physical and logical access across all systems.
- Case Study: Analyzing a scenario where poor offboarding led to a former vendor maintaining access and causing a future Insider Threat incident.
- Archiving all relevant documents for future audit and Regulatory Scrutiny.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
21 Sep 2026	25 Sep 2026	Online	$1,000
21 Sep 2026	25 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com